

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

SEALED

13 JAN 31 PM 1:49

COURT REPORTER  
JOURNAL OF THE CALIFORNIA

BY: DEPT

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

'13 MJ0366

UNITED STATES OF AMERICA, ) Magistrate Case No. \_\_\_\_\_  
 )  
Plaintiff, ) COMPLAINT FOR VIOLATIONS OF:  
 )  
v. ) Title 18, U.S.C., Sec. 1343 - Wire  
 ) Fraud; Title 18, U.S.C.,  
 ) Sec. 1029(a)(3) and (c)(1)(a)(i)-  
MATTHEW WEAVER, ) Access Device Fraud; Title 18,  
 ) U.S.C., Sec. 1030(a)(2)(C) and  
Defendant. ) (b)(2)(B)(ii) - Unauthorized  
 ) Access of a Computer  
 )

The undersigned Complainant, being duly sworn, states:

ALLEGATIONS COMMON TO ALL COUNTS

1. At all times material to this Complaint, defendant Matthew WEAVER was a student at California State University - San Marcos (hereafter, "CSU-SM").

2. At all times material to this Complaint, Associated Students, Inc. (hereafter, "ASI") was the CSU-SM elected student government. ASI elected positions included one president and four vice-presidents. Each of those positions received a stipend. ASI's budget included an \$8,000 stipend for the president and \$7,000 for each vice president.

//



1 usernames and passwords without their knowledge or consent;

2 (c) collected students' stolen CSU-SM account usernames and  
3 passwords in one or more electronic spreadsheets;

4 (d) used the stolen usernames and passwords to access CSU-SM  
5 online accounts and cast CSU-SM students' votes in the March 2012 ASI  
6 election for himself, despite knowing that he was not authorized to  
7 cast those students' votes; and

8 (e) attempted to win the ASI presidency and four vice-  
9 presidencies for himself and his associates, and thereby collect the  
10 \$36,000 in stipends allocated to those offices, on the basis of votes  
11 containing material misrepresentations regarding the voters'  
12 identities and authorization to vote.

13 8. On or about the dates set forth below, in the Southern  
14 District of California and elsewhere, defendant MATTHEW WEAVER, for  
15 the purpose of executing and attempting to execute the above-described  
16 scheme to defraud as to material matters and to obtain money and  
17 property by means of materially false and fraudulent pretenses,  
18 representations, and promises, caused to be transmitted by means of  
19 wire communication in interstate commerce the following signals and  
20 sounds:

<u>COUNT</u>	<u>DATE</u>	<u>DESCRIPTION</u>
22 1	3/14/2012	an electronic ballot sent from the CSU-SM 23 student account of C. C.
24 2	3/15/2012	an electronic ballot sent from the CSU-SM 25 student account of C. L. P.

26 All in violation of Title 18, United States Code, Section 1343.

27 //

28 //

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Count 3

ACCESS DEVICE FRAUD

9. The allegations in Paragraphs 1 through 4 are incorporated and re-alleged by reference in this Count.

10. On or about March 15, 2012, within the Southern District of California, and in and affecting interstate and foreign commerce, defendant MATTHEW WEAVER, knowingly and with intent to defraud, possessed at least fifteen unauthorized access devices, specifically, he possessed an electronic spreadsheet entitled "Fuck ASI alpha" that contained the stolen usernames and passwords for approximately 740 CSU-SM student accounts; in violation of Title 18, United States Code, Sections 1029(a)(3) and (c)(1)(a)(i).

Count 4

UNAUTHORIZED ACCESS OF A COMPUTER

11. The allegations in Paragraphs 1 through 4 are incorporated and re-alleged by reference in this Count.

12. On or about March 15, 2012, within the Southern District of California, defendant MATTHEW WEAVER, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud, in violation of Title 18, United States Code, Section 1343, and access device fraud, in violation of Title 18, United States Code, Sections 1029(a)(3) and (c)(1)(a)(i); all in

//  
//  
//  
//

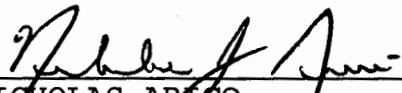
1 violation of Title 18, United States Code, Sections 1030(a)(2) and  
2 (c)(2)(B)(ii).

3

4 This complaint is based on the attached Statement of Facts  
5 incorporated herein by reference.

6

7

  
\_\_\_\_\_  
NICHOLAS ARICO  
Special Agent, FBI

8

9

10 Sworn to me and subscribed in my presence this 30<sup>th</sup> day of January,  
11 2013.

11

12

  
\_\_\_\_\_  
HON. WILLIAM MCCURINE, JR.  
U.S. MAGISTRATE JUDGE

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28



1 some of its web-based services, including VOTE, on its own servers,  
2 the campus's email system is hosted by Google, Inc. Use of CSU-SM  
3 email accounts therefore involves accessing Google's server network.

4 4. This case involved the use of keyloggers. A keylogger is  
5 a small electronic storage device that, when installed between a  
6 keyboard and the computer tower, can record a computer user's  
7 keystrokes without the user's knowledge.

8 5. To date, the FBI has obtained federal search warrants for  
9 a laptop computer, keystroke loggers, and thumb drives seized from  
10 Matthew Weaver by CSU-SM Police Officer Brian McCauley on March 15,  
11 2012. The FBI also obtained a federal search warrant for an email  
12 account controlled by Weaver. Unless otherwise indicated, the  
13 electronic records described below were seized pursuant to these  
14 search warrants or obtained from CSU-SM.

#### 15 **Weaver's Activity**

16 6. In July 2011, Weaver emailed CSU-SM employees a request for  
17 information about ASI's budget. On July 20, 2011, a CSU-SM employee  
18 emailed Weaver an electronic spreadsheet with the requested budget  
19 information. The spreadsheet listed the salaries paid to the ASI  
20 student officers and broke down the ASI activities budget.

21 7. Weaver's laptop contained a PowerPoint presentation that  
22 proposed he and other members of his fraternity run in the March 2012  
23 ASI elections. The presentation included budget information that  
24 appeared to be cut and pasted from the ASI budget spreadsheet emailed  
25 to Weaver in July. The PowerPoint presentation noted that elected ASI  
26 student officers received a salary of between \$1,000 and \$8,000 a year  
27 and had control over a budget of approximately \$300,000. The  
28 presentation proposed that Weaver run for President - which received

1 an \$8,000 stipend, and that four associates run for Vice-President -  
2 which would have paid each one a \$7,000 stipend.

3 8. Browser records for Weaver's laptop show that, in January  
4 and February 2012, he ran search queries for "keylogger," "key  
5 loggers," "keylogger sale," "keygrabber review," "invasion of privacy  
6 cases," "legal issues relating to keyloggers," "jail time for  
7 keylogger," "how to set someone up for a lawsuit," and "how to rig an  
8 election." The browser history also included web pages from Amazon.com  
9 and other online vendors for various brands of keyloggers.

10 9. Email records show that, on February 2, 2012, Weaver  
11 purchased three KeyGrabber keyloggers using a Visa card issued in his  
12 name. The keyloggers were shipped to Weaver's apartment. Weaver's  
13 email account included a folder called "keylogger."

14 10. CSU-SM network administrators determined that Weaver  
15 installed keyloggers on approximately 19 different on-campus public  
16 computers beginning in January 2012. Forensic review of Weaver's  
17 laptop also revealed documents containing key stroke data recorded by  
18 a key logging device. This data included students' usernames and  
19 passwords, as well as the key strokes typed while the users were  
20 monitored by the keystroke-logging device.

21 11. Electronic evidence seized from Weaver's computer shows that  
22 the stolen usernames and passwords were compiled into various  
23 spreadsheets. The most comprehensive of the spreadsheets, entitled  
24 "Fuck ASI alpha," was last modified on March 15, 2012 (the day CSU-SM  
25 police arrested Weaver and seized his computer). The alphabetized  
26 spreadsheet had approximately 740 student usernames and passwords.

27 12. During the ASI election, CSU-SM employees observed  
28 irregularities in the voting. Over the course of several hours



1 beginning on the evening of March 13, 2012, and continuing into the  
2 early hours of March 14, 2012, over 150 votes were cast from a single  
3 off-campus Internet Protocol (IP) address, 70.181.180.100. Subpoenaed  
4 records show that, during the relevant period, Weaver was the listed  
5 subscriber for that IP address.

6 13. Between 12:14 p.m. and 12:39 p.m. on March 14, 2012,  
7 approximately 33 online votes were cast from an on-campus computer  
8 assigned IP address 144.37.93.123. CSU-SM records show that Weaver's  
9 CSU-SM username and password logged into that computer at 12:07 p.m.  
10 and logged off at 12:44 p.m. CSU-SM records also show that Weaver's  
11 laptop connected to a near-by wireless access point at 12:48 p.m. and  
12 was assigned the IP address 144.37.119.117. From 1:18 p.m. to 2 p.m.,  
13 43 votes were cast from that single IP address.

14 14. On the afternoon of March 15, 2012, shortly before the ASI  
15 election ended, CSU-SM employees detected another surge in votes -  
16 approximately 259 - coming from a single IP address, 144.37.239.151.  
17 This IP address originated to a campus computer in CSU-SM's Academic  
18 Hall 204. During this time, Weaver's personal laptop was also logged  
19 into the campus network via a wireless access point associated with  
20 a room, Academic Hall 202, that adjoins Academic Hall 204. (According  
21 to CSU-SM employees, there was no separate wireless for room 204.)  
22 When CSU-SM employees directed Officer McCauley to the computer  
23 assigned IP address 144.37.239.151 to determine who was using it,  
24 Officer McCauley found Weaver seated at the computer. McCauley later  
25 interviewed a student who was in the lab with Weaver and the student  
26 said that Weaver was the only user she recalled seeing at that  
27 terminal while she was in the computer lab.

28

1           15.     Approximately 40 minutes before Officer McCauley found  
2 Weaver, CSU-SM network administrators used a remote desktop function  
3 to pull up the screen of the computer associated with IP address  
4 144.37.239.151, thereby viewing the same screen as Weaver. CSU-SM  
5 records show that, at or about 4:54 p.m., during the time that CSU-SM  
6 network administrators were remotely viewing his computer screen,  
7 Weaver logged into the student account of C. L. P. and used C. L. P.'s  
8 CSU-SM student account to vote for himself. C. L. P. has told the FBI  
9 that he did not authorize Weaver to log-in to his student account or  
10 vote on his behalf.

11           16.     A CSU-SM network administrator, using a cell phone video  
12 function, recorded approximately the last 20 minutes of Weaver's  
13 screen activity. The video shows that Weaver cut and pasted the  
14 usernames and passwords for three CSU-SM students from an Excel  
15 spreadsheet called "Fuck ASI alpha" into the VOTE system and tried to  
16 cast the students' votes. (He got error messages because he cast the  
17 votes shortly after 5 p.m., at which time the election was over.)

18           17.     The video also shows that, shortly after 5 p.m., Weaver  
19 logged into the email account of a CSU-SM administrator, S. G., to  
20 read her emails. There, Weaver saw that a student, C. C., had  
21 complained to S. G. that she could not vote. After pulling C. C.'s  
22 username and password from the "Fuck ASI alpha" spreadsheet, Weaver  
23 logged into C. C.'s CSU-SM email account and sent S. G. an email  
24 retracting the complaint. When S. G., who was logged into email from  
25 a separate computer, responded and asked for clarification, Weaver  
26 sent a response from C. C.'s CSU-SM email account and then, accessing  
27 C. C.'s "Sent" and "Trash" folders, permanently deleted the messages  
28 he had just exchanged with S. G.

1 18. CSU-SM records show that C. C.'s ASI vote was cast on March  
2 14, 2012 from the I.P. address associated with Weaver's home. C. C.  
3 has told the FBI that she did not give Weaver authority to use her  
4 log-in information, to access her email, or to vote on her behalf.

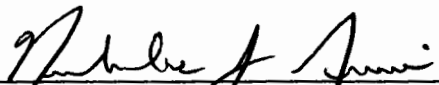
5 19. According to Officer McCauley, when he entered the computer  
6 lab and found Weaver, he saw that the computer used by Weaver was the  
7 only computer whose screen was not visible to the rest of the room.  
8 After a short conversation, wherein Weaver said he was working on a  
9 school project, Officer McCauley arrested Weaver and seized his laptop  
10 computer and bag. Inside the bag, Officer McCauley found keyloggers,  
11 keylogger user guides, and a drawing that resembled a diagram of the  
12 computers in a different CSU-SM computer lab, with arrows next to two  
13 of the computers. After Officer McCauley seized the drawing and  
14 keyloggers, CSU-SM network administrators inspected the campus's  
15 public computer terminals and found keyloggers installed on the two  
16 marked computers in the other computer lab.

17 20. In total, CSU-SM's records tie Weaver to the online votes  
18 cast by approximately 634 CSU-SM students. CSU-SM declined to  
19 announce the election results and instead held a new ASI election.

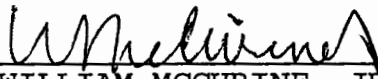
20 21. Evidence seized from Weaver's computer, together with CSU-SM  
21 records, show that Weaver, following his March 15, 2012 arrest,  
22 attempted to incriminate another CSU-SM student, M. L., for the  
23 election fraud. These records show that Weaver created Facebook  
24 accounts for alter egos tied to his own email account, accessed  
25 M. L.'s Facebook account, and took a screen-shot of M. L. and these  
26 fictitious alter egos having a group chat in which they acknowledged  
27 smearing Weaver's reputation. Weaver, using a fake identity and email

28

1 - crissanmarcos@yahoo.com - emailed the screenshot to local reporters  
2 on March 19, 2012.

3   
4 \_\_\_\_\_  
5 NICHOLAS ARICO, Special Agent  
6 Federal Bureau of Investigation

6 SUBSCRIBED and SWORN to before me on January 30 \_\_\_\_\_, 2013.

7   
8 \_\_\_\_\_  
9 HON. WILLIAM MCCURINE, JR.  
10 UNITED STATES MAGISTRATE JUDGE

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28